STATE OF ALABAMA

Information Technology Standard

Standard 610-01S1: Cyber Security Awareness and Training

1. INTRODUCTION:

A key element in a successful cyber security program is user awareness and training. Security across multiple hardware and software platforms requires security-aware users as well as a well-trained technical staff.

2. OBJECTIVE:

Ensure all employees receive timely cyber security awareness and training, appropriate to their roles and responsibilities, to increase awareness of information security risks, increase technical competence, and ensure compliance with information security policies and standards.

3. SCOPE:

These requirements apply to all personnel (State of Alabama employees, contractors, vendors, or business partners) responsible for the security awareness and training of State of Alabama information system resource users and technical staff.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) in Special Publication 800-53: Recommended Security Controls for Federal Information Systems, the following requirements apply to State of Alabama cyber security awareness and training programs:

4.1 CYBER SECURITY AWARENESS AND TRAINING PROGRAM

Organizations shall develop, disseminate, and periodically review/update a cyber security awareness and training program consisting of:

> (i) a formal, documented, cyber security awareness and training plan that addresses roles, learning objectives and methods, schedule, and resources; and
>
> (ii) formal, documented procedures to facilitate the implementation of the cyber security awareness and training plan and associated security awareness and training controls (as defined in State standards). Security awareness and training procedures shall be developed for the security program in general and (when required) for a particular information system.

NIST Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model, and NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program provide guidance on developing security awareness and training programs.

4.2 SECURITY AWARENESS

Ensure all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.

Determine the appropriate content of security awareness level training based on the specific requirements of the organization and the information systems to which personnel have authorized access.

Cyber security awareness programs shall be consistent with the requirements in 5 C.F.R. Part 930, Subpart C and with the guidance in NIST Special Publication 800-50.

Security Awareness Topics include (but are not limited to):

- Policies and Standards and where to find them
- Password usage and management – creation, frequency of changes, and protection
- E-mail usage – handling attachments, prohibited use, mass mailings
- Web usage – access, prohibited use, monitoring of user activity
- Malware Protection – viruses, worms, Trojan horses, and other malicious code
- Vulnerability Management – timely application of system patches
- Spam
- Social engineering
- Incident response – reporting and handling
- Physical Security – facility access, visitor control, environmental risks, etc.
- Desktop security – use of screensavers, restricting visitors' view of information on screen (preventing "shoulder surfing"), allowed access to systems
- Laptop security – both physical and information security issues
- Handheld device security – both physical and wireless security issues
- Individual accountability – identification and authentication; access to systems and data
- Access control issues – least privilege, separation of duties, etc.
- Personally owned systems and software at work or connecting remotely
- Software licensing and use
- Data backup and storage
- Information Protection – confidentiality concerns and controls
- Encryption – transmission and storage of sensitive/confidential information
- Information System Disposal – property transfer, media sanitization

4.3 SECURITY TRAINING

Identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorizing access to the system and at least annually thereafter.

Determine the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access.

Ensure system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties.

Cyber security training programs shall be consistent with the requirements in 5 C.F.R. Part 930, Subpart C and with the guidance in NIST Special Publication 800-50.

4.4 SECURITY TRAINING RECORDS

Document and monitor individual information system security training activities including basic security awareness level training and specific information system security training.

5. DEFINITIONS:

AWARENESS vs. TRAINING (as defined in NIST Special Publication 800-16):

> *"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance."*

TRAINING LEVELS (as defined in 5 C.F.R. Part 930.301):

(1) **Awareness level training** creates the sensitivity to the threats and vulnerabilities and the recognition of the need to protect data, information, and the means of processing them.

(2) **Policy level training** provides the ability to understand computer security principles so that executives can make informed policy decisions about their computer and information security programs.

(3) **Implementation level training** provides the ability to recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement agency security policies.

(4) **Performance level training** provides the employees with the skill to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 610-01: Security Awareness and Training

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	1/12/2007	